## REMARKS

The Office Action dated May 25, 2005 has been received and carefully noted. The above amendments and the following remarks are submitted as a full and complete response thereto.

Claims 1, 13, 23 and 29 are amended to particularly point out and distinctly claim the subject matter of the invention. Applicants respectfully request entry of the above amendments because the amendments place the application in condition for allowance. No new matter is added.

Applicants are grateful for the courtesies extended to the Applicants' representative by Examiner Davis during the personal interview on July 14, 2005. Applicants' summary of the interview is incorporated in the following remarks. Claims 1-32 are respectfully submitted for consideration.

Claims 1-32 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Number 6, 659,861 to Faris et al. (Faris). Applicants respectfully submit that claims 1-32 recite subject matter which is neither disclosed or suggested by Faris.

Claim 1, upon which claims 2-12 depend, recites a method of preventing upload overloads of data from a plurality of clients at different locations within a network to a common destination server in the network. The method includes generating a unique identifier corresponding to and dependent on data that each client intends to send to the common destination server, the unique identifier being smaller in size than the data of the client. The method further comprises separately transmitting the unique identifiers from each client to at least one authenticator trusted by the common destination server, wherein the at least one authenticator is a component of the destination server, and separately time-stamping the unique

identifiers as received by the authenticator. The method further comprises separately sending back to each client a message, digitally signed by the authenticator, with the unique identifier sent by that client and the corresponding time-stamp, each client then sending its data towards the common destination server. Further, the method comprises the common destination server using the unique identifier for the data provided by each client to confirm that the data provided by each client existed as of the corresponding time-stamp and to insure that the data has been unaltered after the corresponding time-stamp.

Claim 13, upon which claims 14-22 depend, recites a method of preventing upload overloads of data from a plurality of clients at different locations within a network to a common destination server n the network. The method comprises generating a unique identifier corresponding to and dependent on data that each client intends to send to the common destination server, the unique identifier being smaller in size than the data of the client and separately transmitting the unique identifiers from each client to at least one authenticator trusted by the common destination server, wherein the at least one authenticator is a component of the destination server. The method further includes separately sending back to each client a message, digitally signed by the authenticator, with the unique identifier sent by that client and each client then forwarding its data to the common destination server via proxy upload servers remote from the common destination server. The method further includes the common destination server using the unique identifier for the data provided by each client to confirm that the data provided by each client has been unaltered after the generation of the unique identifier.

Claim 23, upon which claims 24-28 depend, recites a method of preventing upload overloads of data from a plurality of clients at different locations within a network to a

common destination server in the network. The method includes providing a common destination server in a network, the common destination server set up to receive data from a plurality of clients. The method further includes providing a plurality of upload proxy servers remote from the common destination server. The method further includes each client sending data, which is intended for the common destination server, to at least a corresponding one of the upload proxy servers. Further, the method includes sending a message, which is smaller in size than the data of a client, to the common destination server to indicate that the common destination server needs to check the corresponding one of the upload proxy servers , and upload data from the corresponding one of the upload proxy servers. Further, the method includes having the common destination server upload the data of a client at some time after the message such that a plurality of clients trying to send data to the common destination server at essentially the same time, is less likely to overload the common destination server and its connection to the network.

Claim 29, upon which claims 30-32 depend, recites a system for preventing upload overloads of data from a plurality of clients at different locations within a network to a common destination server in the network. The system includes a common destination server in a network, the common destination server set up to receive data from a plurality of clients. The system further includes an id generator operable to generate a unique identifier corresponding to and dependent on data that each client intends to send to the common destination server, the unique identifier being smaller in size than the data of the client. The system further includes each client having a sender for separately transmitting the unique identifier from that client. Further, the system includes at least one authenticator trusted by the common destination

server, the authenticator having a time-stamper for separately time-stamping the unique identifiers as received by the authenticator, the authenticator having a sender for separately sending back to each client a message, digitally signed by the authenticator, with the unique identifier sent by that client and the corresponding time-stamp wherein the at least one authenticator is a component of the destination server. In the system, the common destination server includes a checker that uses the unique identifier for the data provided by each client to confirm that the data provided by each client existed as of the corresponding time-stamp and to insure that the data has been unaltered after the corresponding time-stamp.

The invention prevents or minimizes the likelihood of the destination server becoming overloaded due to a plurality of network clients that wish to upload files to the destination server. Overload is prevented by the clients sending a unique identifier to an authenticator which time stamps the identifier, digitally signs the identifier and sends a message to the client. The client sends time-stamped messages to the destination server which indicate that a file is ready to be uploaded to the destination server. The claims of the present invention, recite features that are neither disclosed or suggested in the prior art.

The Office Action alleged that Faris disclosed all of the features of the pending claims. Faris discloses an internet-based system for enabling a time-constrained competition among a plurality of participants over the internet. Faris discloses a plurality of Global Synchronization Unit-enabled client machines, each with a Global Synchronization Unit (GSU). Further, at column 24 lines 34-38, Faris discloses that a client machine is connected to a global synchronization unit (GSU) and at column 36 lines 54-58 discloses that the GSU (alleged authenticator) "generates digitally signed time and space stamp for the response."

As discussed during the personal interview, this is in contrast to the features recited in independent claims 1, 13 and 29. According to the present invention and as recited in claims 1, 13 and 29 and their corresponding dependent claims, the authenticator is a component of the destination server (see Fig. 5 and page 13 line 25 – page 14 line 4). Thus, the authenticator portion of the destination server sends data with digital signatures to the client. Therefore, the unique identifier and digital signature are performed at the destination server. As discussed above, Faris teaches that the GSU is a part of the client device.

It is respectfully submitted that since claims 2-12, 14-22 and 30-32 depend from claims 1, 13 and 29 respectively, these claims are allowable at least for the same reasons as claims 1, 13 and 29.

Regarding claim 23, as discussed above claim 23 recites the feature of sending a message, which is smaller in size than the data of a client, to the common destination server to indicate that the common destination server needs to check the corresponding one of the upload proxy servers, and upload data from the corresponding one of the upload proxy servers.

As discussed during the personal interview, Faris fails to disclose or suggest this feature. While Faris discloses sending a separate message that is a compilation of sets of data from multiple client machines (column 38 lines 39-52), Faris does not disclose that the message is an indication to check the proxy server and upload data from that proxy server, as recited in claim 23.

It is respectfully submitted that since claims 24-28 depend from claim 23, these claims are allowable at least for the same reasons as claim 23.

At least in view of the above, it is respectfully submitted that the cited reference fails to

disclose or suggest all of the features recited in claims 1-32. Accordingly, withdrawal of the rejection of claims 1-32 under 35 U.S.C. §102(e) is respectfully requested.

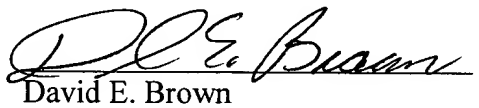
**CONCLUSION**

Therefore, Applicants respectfully further submit that claims 1-32 of the present application contain allowable subject matter, respectfully request that all claims pending in the present application be allowed, and further request that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



David E. Brown
Registration No. 51,091

**Customer No. 32294**
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DEB:mm